SANDIA REPORT

SAND2004-2109
Unlimited Release
Printed June 2004

International Biosecurity Symposium:
Securing High Consequence Pathogens and Toxins

Symposium Summary

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.doe.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

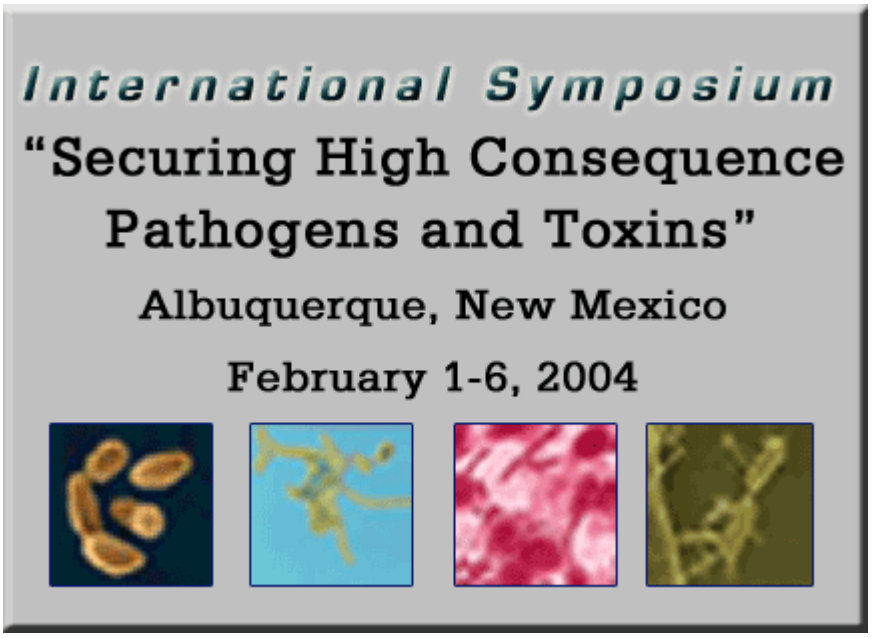

Table of Contents

Note:
Symposium presentations and electronic versions of this summary may be found by visiting Sandia's biosecurity website, www.biosecurity.sandia.gov.

Introduction

The National Nuclear Security Administration (NNSA) Office of Nonproliferation Policy sponsored an international biosecurity symposium at Sandia National Laboratories (SNL). The event, entitled "Securing High Consequence Pathogens and Toxins," took place from February 1 to February 6, 2004 and was hosted by Dr. Reynolds M. Salerno, Principal Member of the Technical Staff and Program Manager of the Biosecurity program at Sandia.[1] Over 60 bioscience and policy experts from 14 countries gathered to discuss biosecurity, a strategy aimed at preventing the theft and sabotage of dangerous pathogens and toxins from bioscience facilities.

Presentations delivered during the symposium were interspersed with targeted discussions that elucidated, among other things, the need for subsequent regional workshops on biosecurity, and a desire for additional work toward developing international biosecurity guidelines.

Symposium Purpose

During the August 2003 Experts Group Meeting of the Biological Weapons Convention (BWC), which focused on "national mechanisms to establish and maintain the security and oversight of pathogenic microorganisms and toxins," it became evident that additional discussions concerning pathogen and toxin security (biosecurity) could be beneficial to the international community. A follow-up symposium, designed by the NNSA to share information and clarify international perspectives on biosecurity, was organized to facilitate a continued dialogue. SNL, a leader in designing and implementing biosecurity in the United States, hosted the event.

The symposium had three broad goals:

1) To present the United States' experiences in implementing biosecurity.
2) To elicit from the international participants their interpretations and concerns about biosecurity.
3) To set biosecurity in the context of biological weapons non-proliferation and counter-bioterrorism.

Throughout the symposium, audience participation was strongly encouraged. Discussion sessions were organized each day; including hour-long question and answer sessions following each presentation on days three and four. The final day was devoted a round-table discussion.

[1] Additional members of the Sandia Biosecurity team include: George Baldwin, Natalie Barnett, Susan Caskey, Daniel Estes, Jennifer Gaudioso, Lauren Hickok, John Milloy, Susan Rivera, and Nora Tankersley.

Summary of Presentations and Discussions[2]

Day One, Monday, February 2, 2004

A variety of governmental and non-governmental institutions presented a broad spectrum of biological weapons related issues.

Sandia National Laboratories Introduction

Dori Ellis, M.S., Sandia National Laboratories

Dori Ellis, Director of the International Security Center at SNL, welcomed Symposium participants. She introduced SNL and its International Programs, specifically the Labs' nonproliferation initiatives.

Ms. Ellis explained how SNL helps the United States secure a peaceful and free world by creating technologies and methodologies that support US policy decisions that are aimed at reducing the threat of weapons of mass destruction (WMD) proliferation. SNL's International Security Programs (ISP) division furthers this goal by developing technology systems through international cooperation. The ISP works for WMD nonproliferation in three functional areas: nuclear nonproliferation and combating terrorism, regional security, and biological weapons (BW) nonproliferation.

Historical Trends and the Biological Weapons Threat

Michael Moodie, The Chemical and Biological Arms Control Institute (CBACI)

In his presentation, Mr. Moodie reviewed the historical record of biological weapons development and use. He concluded his presentation by assessing the current biological warfare and bioterror threat.

The first documented use of disease-causing microorganisms as weapons occurred in 1346 when attacking Tartars catapulted plague-infected corpses over the city walls of Kaffa, Ukraine. Since then, biological weapons have been used in only a limited number of isolated cases, and have characteristically involved attempts to cause casualties among civilian populations.

Although BW use has been relatively rare, state-sponsored biological weapons programs proliferated around the world throughout the 20th Century. These programs reached their apex with the Soviet Union's Biopreparat weapons program, which was greatly expanded in the 1970s and 80s, despite the USSR's accession to the BWC.

[2] The summaries provided herein reflect the content presented by the speakers; every attempt has been made to ensure these summaries retain the speakers' perspectives. The views expressed are not necessarily those held by the USG, NNSA, or SNL.

Recently, terrorists, terrorist organizations (including al Qaeda), and other malevolent persons and groups have shown increasing interest in producing and/or gaining access to biological weapons materials. Fortunately, these efforts have generally met with limited success. The notable exception being the 2001 anthrax attacks in the US, which killed five civilians and injured 21.

The Biotechnology Revolution and the Biological Weapons Threat

Tara O'Toole, MD, MPH, Center for Biosecurity at the University of Pittsburgh Medical Center

Dr. O'Toole advanced the thesis that catastrophic-level biological attacks are not only possible; they are, in point of fact, likely to occur. Because of their potential to cause a mass casualty event, biological weapons should be considered a strategic threat – on par with thermonuclear weapons – and should be treated as such by policymakers and microbiologists. The chances that biological weapons will be used are high because it has been proven that they work, because the knowledge and materials necessary to produce and deploy BW are widespread, and because the world's epidemic response systems are vulnerable to failure if overburdened.

Aside from considerable beneficial advances, recent developments in the biosciences have created new threats. Now scientists can increase the virulence of pathogens and can synthesize viruses with commercially available equipment and publicly available information. New delivery technologies such as micro-encapsulation, carrier beads, and aerosols – all legitimate bioscience advances – will make it easier to deploy potentially catastrophic BW in the future.

Because of these scientific and technological developments, the actual pathogen located in a legitimate facility is no longer required for biological weapons proliferation. Knowledge is now the most valuable asset for a bioweaponeer. As a result, securing pathogens and toxins from theft is not an effective strategy to counter the bioweapons threat. Policymakers should invest in biodefense rather than in biosecurity.

Although there are many challenges to achieving a sufficient biodefense system, it is a necessary undertaking in light of today's (and tomorrow's) biological weapons threat. The possibility that biological weapons will be used as a WMD grows every day. Tightening the security surrounding laboratory-based pathogens and toxins is not a viable answer to address this threat. Preventing the severity of an infectious disease epidemic through research and development into countermeasures should be the priority of scientists and policymakers around the world.

Pathogen Security and the Biological Weapons Convention

Gregory Stewart, Ph.D., Bureau of Arms Control, Office of Chemical and Biological Weapons, US Department of State

Following the rejection of the Verification Protocol in 2001, Member States of the BWC agreed to meet annually until 2006 to discuss alternative measures to strengthen the Convention. The 2003 series of meetings addressed national BWC-implementing legislation and pathogen security. Dr. Stewart focused his presentation on pathogen security within the context of the BWC.

Member States of the BWC came to a variety of conclusions during the 2003 meetings. First, it was believed by some States Parties that the international community – with guidance from the WHO – should establish a list of dangerous pathogens to be controlled. Second, it was proposed that each Member State identify or create a national authority to oversee pathogen security. Third, it was emphasized that States Parties without BWC-implementing legislation should create such legislation. And fourth, that this legislation, once in place, should be rigorously enforced.

Pathogen security is a global problem. Therefore, it is appropriate that it be addressed within an international convention such as the BWC. Also, the BWC is a convenient forum in which to promote biosecurity because it allows States Parties with questions concerning the implementation of biosecurity to contact other countries that have addressed this issue.

Options for Reducing the Threat

Elizabeth Cameron, Ph.D., Bureau of Nonproliferation, US Department of State

Dr. Cameron presented an overview of the independent research conducted by Anne Harrington, Deputy Director of the Office of Proliferation Threat Reduction, US Department of State.

The threat of a biological weapons attack caused by a non-state actor is recognized throughout US Government. Unfortunately, solutions to lessen this danger have not been adequately formulated. A new methodology, distinct from traditional forms of arms control, must be introduced to reduce the threat of bioterrorism. This new technique should focus on two distinct goals: First, to reduce the potential bioterrorist's capabilities of creating a weapon, and second, to limit the public health consequences if such a weapon were successfully deployed.

The first of these goals can be achieved by controlling access to the three necessary components of a biological weapon: the pathogen or toxin, the expertise, and the technology. The second can be accomplished by strengthening the global Public Health system by encouraging communication between health care communities,

expanding international cooperation in disease surveillance and diagnostics, and facilitating research and development into technologies that combat bioterrorism.

Biomedical Countermeasures

Lt. Col. Ross H. Pastel, Ph.D., US Army Medical Research Institute of Infectious Diseases (USAMRIID)

Lt. Col. Pastel, Deputy Commander of safety, biosurety, and security at USAMRIID presented an overview of the institute's capabilities. These capabilities span the full spectrum of biological defense techniques, from disease prevention to detection and treatment.

USAMRIID houses the largest collection of BSL-4 containment space in the US, including a BSL-4 patient care suite. These high-containment areas facilitate the institute's primary mission of providing medical solutions to protect war fighters and, by extension, the civilians of the US. USAMRIID conducts absolutely no classified research and seeks to publish all of its research.

USAMRIID has developed many vaccines and therapeutics against potential biological weapons agents. Further, the institute is equipped with state-of-the-art laboratory and field diagnostic capabilities to enhance the US's ability to identify infectious diseases and investigate outbreaks around the world.

Veterinary Infectious Diseases, New Technologies and the Future

Keith Murray, Ph.D., National Animal Disease Center, US Department of Agriculture (USDA)

Dr. Murray noted that agriculture is a $100 billion industry in the US and emphasized that it is potentially vulnerable to certain types of biological weapons attacks. Recognizing this fact, USDA has shifted its focus from promoting animal and plant productivity to preventing and controlling the spread of infectious disease.

Since many of the diseases that affect animal health are also transmissible to humans, veterinary diagnostics are an important link in the biodefense chain. USDA uses a variety of interconnected strategies to help prevent, detect, and contain infectious disease outbreaks; including biosecurity, import and export controls, PCR-diagnostics, and disease surveillance. These techniques are equally applicable to both natural disease outbreaks and bioterrorism attacks.

Bio-Forensics

Jill Trewhella, Ph.D., Bioscience Division, Los Alamos National Laboratories (LANL)

Dr. Trewhella introduced DNA-based bio-forensics as one the tools utilized by the biodefense industry to help determine a pathogen's origin by mapping its genome. Bio-forensics was used to evaluate *bacillus anthracis* samples from Russia following

the 1979 accident in Sverdlovsk, USSR. The technique was also used in Iraq by the United Nations Special Commission (UNSCOM) members, and after the anthrax attacks on the US in 2001.

In the past, LANL has openly published many different genome sequences, but the new US Select Agent Rule has confused what is publishable and what is not. Since the Rule went into effect, scientists have generally erred on the side of caution regarding the publication and distribution of Select Agent information.

Next Generation Sensors

Thomas Bevan, Ph.D., Georgia Tech Center for Emergency Response Technology

Dr. Bevan suggested that expedited deployments of countermeasures could mitigate the effects of a biological weapons attack by preventing its development into an epidemic. Biosensors accelerate response time by quickly determining if a biological agent has been used in an attack and, if so, the nature of that agent. Sensors constitute an important tool for first responders.

Sensor technology is still in its early stages, and existing sensors are either too bulky or too expensive to be used effectively on a wide scale. The US Government should fund future research into creating user-friendly, portable, and inexpensive sensors for use by first responders across the US.

Discussion

During the first day's discussions, a variety of topics were raised that would continue to appear throughout the conference. The US Select Agent Rule, in particular, was a major theme for debate. Some members of the audience – both international and from the United States – worried that the US Select Agent Rule had caused more problems that it had solved. For instance, it was thought by many that the Rule was obstructing critical diagnostic work, especially during the international transfer of Select Agent samples. Also, despite the significant amounts of new funding for bioscience research involving Select Agents there was some concern that the US Select Agent Rule was driving scientists and prospective scientists away from critical research involving regulated agents. Many suggested that this could have long-term and undesirable effects on the development of vaccines and therapeutics for some common and deadly infectious diseases.

There is no unique definition of "biosecurity," and the different participants used the term in a variety of manners. Some participants used "biosafety" and "biosecurity" interchangeably, while others defined biosecurity as protecting humans and agriculture from infectious disease. Sandia National Laboratories defines biosecurity as protecting dangerous pathogens and toxins from theft and sabotage in a legitimate laboratory and inter-laboratory (transport) setting. This definition became accepted for the purposes of the symposium; however, agreement on whether SNL's definition of biosecurity was the proper use of the term was never unanimously agreed upon.

Day Two, Tuesday February 3

The events of the day were divided into two sections. The morning was dedicated to international biosecurity presentations, which were followed by a panel discussion. The afternoon was devoted to poster presentations that focused on counter-biological weapons technologies.

Biosecurity: The UK Response
Guy Collyer, National Counterterrorism Security Office, United Kingdom

Although the terrorist events of September 11, 2001, and the subsequent anthrax attacks occurred within the United States, they caused dramatic policy shifts around globe. The UK for example, in response to these attacks, passed the Anti Terrorism Crime and Security Act of 2001. This legislation – an omnibus counterterrorism bill – contains a section devoted to securing the potentially dangerous pathogens and toxins found on the Australia Group's Common Control Lists.[3]

According to Mr. Collyer, the UK is adhering to a mandate provided by the Anti Terrorism Act by beginning to implement biosecurity at the nation's bioscience laboratories. Implementation has been pursued incrementally and has started with a "hearts and minds" campaign. This campaign is introducing and acclimating research scientists – who traditionally have not been accustomed to security regulations – to the national security rationales and technical mechanisms of biosecurity.

It is Mr. Collyer's opinion that successful implementation of biosecurity requires the understanding and cooperation of both the scientific community at large and the individual researchers that must interact with biosecurity on an every day basis. Biosecurity system designers in the United Kingdom have been working with members of the scientific and research communities to ensure the implementation of a more realistic and viable version of biosecurity. Members involved in the UK's biosecurity planning understand that biosecurity must not create research conditions that are overly restrictive to the scientists. Concurrently, these scientists must begin to appreciate the national security benefits of protecting dangerous biological materials from theft.

Only after the importance of biosecurity has been impressed upon the microbiological community will they begin to support the implementation of specific biosecurity technologies and policies.

[3] The Australia Group (AG) is an informal assemblage of 34 countries that aims to minimize the risk of assisting chemical and biological weapon proliferation by harmonizing export-licensing practices. The AG has compiled three Common Control Lists of pathogens and toxins that should be export controlled by Member States. These lists may be found on the AG website, www.australiagroup.net/en/agcomcon.htm.

Integrated Biological Attack Response System in Poland: Model and Reality

Janusz Kocik, MD, Ph.D., Military Institute of Hygiene and Epidemiology, Poland

Dr. Kocik emphasized that preventing epidemic disease is a priority for Poland. To facilitate this goal, the Polish military has designed and is beginning to implement a biodefense program that is integrated into the civilian public health infrastructure. Features of this program – named the Integrated Biological Attack Response System – include creating seven mobile biological response forces within the Polish Armed Forces, improving diagnostic capabilities of BSL-3 laboratories, and strengthening and expanding Poland's disease surveillance system.

When the difficulties associated with implementation – especially the financial burdens – have been solved, the program will significantly expand Poland's disease diagnosis and health surveillance capabilities.

Biological Threats and Biosecurity Efforts in Indonesia

Fransiscus Halim, MD, MS, National Institute of Health Research and Development, Ministry of Health, Indonesia

Dr. Halim noted that the definition of "biological threats" is different in Indonesia than in the US. Anthrax, plague, tuberculosis, malaria, typhoid, and Dengue haemorrhagic fever are all diseases endemic to Indonesia. Outbreaks of these diseases are common, occurring almost every year. Indonesia's public health system – already strained by its limited resources – has placed as its priority the control of these and other infectious diseases. Bioterrorism is not perceived as a specific threat in Indonesia. Thus, it would be difficult to reallocate funds from existing infectious disease detection, prevention, and control techniques to counter-bioterrorism initiatives, including biosecurity.

Indonesia defines biosecurity broadly. Biosecurity encompasses biosafety, import controls, and outbreak response training. Biosecurity is not limited to protecting laboratory-based pathogens and toxins from theft. Dr. Halim argued that such a narrow strategy has limited value in Indonesia, where dangerous pathogens are not only located in laboratories, but can also be found readily in nature.

Biosecurity: South African Approach

Benjamin Steyn, MD, South African Military Health Service, South Africa

According to Dr. Steyn, South Africa – as well as many other nations around the world – uses the terms biosafety and biosecurity interchangeably. Biosafety has been applied well throughout the nation and, at the present, South Africa has no plans to augment laboratory biosafety with new pathogen-specific security and oversight mechanisms.

South Africa believes strongly in biological weapons nonproliferation. South Africa has passed WMD-related legislation including export controls and harsh penalties for actions in contravention of the BWC. Although South Africa does not currently have legislation establishing security policies for pathogens and toxins or plans to adopt such legislation, if such legislation were to be drafted it would need to take into consideration the realities of the research environment that would be affected. Any security guidelines that appear would need to be developed to address the perceived bioterror or biological weapons proliferation threat (which is low in South Africa). Further, any rules created should not be overly burdensome to the microbiological sciences, the rules should be cost-effective and sustainable within the microbiological community.

Any security methodology must be based around a list of the pathogens and toxins that require protection. The Australia Group's Common Control Lists would provide a suitable biosecurity reference.

Biosecurity and Biosafety Practices

Antony Della Porta, Ph.D., Biosecurity and Biocontainment International Consultants Pty Ltd, Australia

According to Dr. Della Porta Australia defines biosecurity as "the prevention of deliberate misuse of biological pathogens and toxins." Therefore, although protecting pathogens and toxins from theft is not the entirety of biosecurity, it is one useful aspect of it. Because biosafety and biosecurity share the goal of preventing a release (either accidental or intentional) of infectious agents from a laboratory, biosecurity should be considered a component of biosafety.

There are overlaps with the practices and procedures used in biosafety with those used to prevent the theft of pathogens and toxins. For example, access controls on high-containment laboratory entryways are designed to ensure that only well-trained and appropriate individuals gain access to the laboratory. Also, decontamination and disinfection practices limit the chances that viable pathogens will be removed from the containment area. Thus, biosafety and preventing the theft of pathogens have many similar and overlapping features.

Implementation of Biosecurity in the United States

Janet Nicholson, Ph.D., National Centers for Infectious Disease, Centers for Disease Control and Prevention (CDC), United States

The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 revamped and expanded the 1996 Select Agent Rule to include pathogen and toxin security. These new security requirements include, among other things, the registration of facilities that house Select Agents, registration of persons with access to Select Agents, and the regulation of the transfer of Select Agents.

Dr. Nicholson explained that, in compliance with the new US Select Agent Rule, each facility must conduct a security risk assessment, including the identification of all Select Agents within the premises. In addition, a background check must be completed for each individual who has access to a Select Agent. Finally, a security plan must be implemented, emergency response plans must be drafted, and security training must be initiated.

Currently, implementation of the Select Agent Rule is underway at the CDC and other microbiological laboratories around the country. The implementation of the Rule is being met with mixed opinions regarding its ability to effectively protect pathogens and toxins from theft and sabotage while maintaining the transparency and expediency that is necessary in microbiological research.

Discussion

Tuesday morning's presenters formed a panel to answer questions from the audience. Many salient topics arose, including questions regarding the creation of pathogen lists and the safe and secure transportation of infectious disease-causing pathogens.

Many of the participants noted that creating country-specific lists of dangerous pathogens and toxins to be regulated might be a necessary task. Most countries, in fact, have already created such lists for export control or biosafety purposes. Participants differed in their views on how inclusive pathogen lists should be. There were calls for both long lists and short lists, with justifications for both.

Long lists, such as the Australia Group's Common Control Lists and the United States' Select Agent List, are useful in different ways. First, a long list may act to obfuscate a nation's true agents of concern by including agents that are not necessarily suitable for bioweaponization, along with those that are. A short list that includes only weaponizable agents could create a target list for potential bioweaponeers. Second, because the Australia Group has already created comprehensive lists of pathogens and toxins that many nations draw upon to determine their export controls, using the Common Control Lists for biosecurity could be more convenient than creating an original list. Third, if biosecurity were implemented in such a way that the specific impacts on protected agent research were minor, creating a long list would be the responsible action for a nation to take. Creating a long list in this case would protect a wide variety of potentially dangerous microorganisms and toxins without hindering research on these agents.

Creating a long list of agents to protect also has drawbacks. If biosecurity were implemented in a way that research on protected agents was significantly hindered, long lists may create overly burdensome research environments, which could detract from legitimate research on a broad spectrum of pathogens and toxins. If microbiologists were deterred from working with regulated agents, a long list would only exacerbate the problem. Also, there is the general opinion that very few – perhaps less than 20 – pathogens truly constitute a threat to public or agricultural

health, and even fewer still that could be used effectively as a biological weapon. Thus, a large list that includes three or four times this many agents would create an inefficient and wasteful allocation of biosecurity resources. In many countries resources available to biosecurity will be limited.

Some participants expressed the view that different levels of biosecurity should be applied based on the biosafety level of the pathogens. Thus, a BSL-4 agent would receive the highest levels of security while BSL-2 agents would receive considerably less security. Arguments against this approach include the fact that, while some BSL-4 agents pose a severe threat to human health, they may not contain the attributes that make them easy to deploy as a weapon. However, some BSL-2 agents do. Security based on biosafety levels is inappropriately applied in cases where this is true.

Tuesday's discussion session also raised the issue of the safe and secure transfer of dangerous pathogens and toxins. While safety-oriented packing and handling guidelines are well established by the United Nations and the International Air Transport Association, there are currently no similar guidelines on the *secure* transport of pathogens.

Further, there was a general concern over the issue of informal "vial in pocket" (VIP) transfers of infectious substances. It was stated that this practice is far too common and that it should be prevented and punished when detected.

Days Three and Four, Wednesday and Thursday February 4 & 5

The presentations on days three and four were given by members of Sandia's biosecurity team. Sandia shared its experience in designing and implementing biosecurity systems, recognizing that the implementation of biosecurity in the United States will differ from the implementation of biosecurity in other countries. Therefore, these presentations were not intended to provide "the answer," but rather, were intended to be used as a reference point from which to begin an international biosecurity discussion. Each presentation of days three and four was followed by an hour-long question and answer discussion session.

Biosecurity Methodology

Reynolds Salerno, Ph.D., Sandia National Laboratories, United States

Microbiological laboratories house certain pathogens and toxins that, if diverted, could be used in biological weapons programs. Biosecurity is a set of procedures and technologies that aims to protect these dangerous materials from theft and sabotage.

Because biosecurity aims to prevent the illicit diversion of dangerous pathogens and toxins – one of the potential paths to biological weapons proliferation – it should be considered an important component of a broad nonproliferation strategy.

There are, however, fundamental difficulties in implementing biosecurity. One of the most significant obstacles is overcoming the impression – generally held by

bioscience researchers who are not accustomed to security procedures – that biosecurity is intrusive, counterproductive, restrictive, or insulting. Creating a "biosecurity culture" by illustrating how biosecurity can be useful and not overly burdensome is one of the primary tasks to be accomplished by biosecurity system designers.

Creating a "biosecurity culture" starts with helping the laboratory scientists understand the national security rationale for biosecurity. Concurrently, the experts responsible for instituting biosecurity at a site must understand the public health necessities and unique nature of bioscience. This common understanding can only occur when the two groups communicate freely with one another.

Sandia practices a risk management approach to biosecurity. This strategy assigns the highest levels of security only to those materials that pose the highest national security risk. Risk is determined by weighing a combination of the consequences associated with an asset (pathogen or toxin) being used as a biological weapon, and the threat potential of that asset being stolen for use as an effective weapon. Sandia recommends the allocation of limited security resources preferentially, i.e., to those few pathogens and toxins that would be most attractive to an adversary intent on pursuing bioterrorism. Sensitive security information and moderately dangerous pathogens and toxins would receive proportionally lower levels of protection under this biosecurity methodology.

Sandia has identified six interconnected components of biosecurity: 1) physical security, 2) personnel security, 3) material control and accountability, 4) transfer security, 5) information security, and 6) program management. Each of these topics was discussed in separate presentations.

Discussion

There was a general concern that biosecurity measures will be forced upon the scientific community by policymakers who may not fully understand the nature of microbiological research; that is the perceived situation in the US with regard to the Select Agent Rule. If this were to happen, the security policies may be out of line with the procedural realities of the laboratory and could cause more harm than good. Specifically, there was apprehension that the limited funds allocated to endemic disease research would be diverted toward security implementation or other counter-bioterrorism programs. Further, the "top down" approach may institute security technologies and policies that, because of their maladaptation to the realities of microbiological research, would create a false sense of security among policymakers. There was a common insistence that the scientists themselves must be intimately involved in creating biosecurity if it is to be an effective and accepted practice.

The "bottom up" approach, where scientists largely influence the policymaking, was the method in which biosafety standards were promulgated, and thus has successful precedent within the microbiological community.

The divide between biosafety and biosecurity was debated. Some participants viewed biosecurity as a subset of biosafety. Others saw it as a separate entity. Sandia believes that, while the two are necessarily inter-related and must work to strengthen one another, there are fundamental differences between the two. Definitionally, biosafety guards against the *accidental release* of pathogens and toxins to protect individuals and the environment. Biosecurity guards against the *deliberate unauthorized removal or destruction* of pathogens and toxins by protecting these materials from those individuals who may pose a threat.

There was prolonged discussion over the issue of agent prioritization. Sandia believes that certain attributes should be weighed to determine which agents should receive the highest levels of protection. Those attributes include: the ease of weaponization (which is a summary attribute incorporating the environmental hardiness, the degree of processing required in order to disseminate the material, and the ease with which the material is grown), the availability of the agent, the availability of countermeasures, as well as the more traditional disease-related components including the agent's infectivity, pathogenicity, lethality, and transmissibility. However, these factors are to some degree subjective and no unanimity exists on exactly which pathogens pose the greatest security risks. Thus, agent prioritization should be determined on a country-by-country or even lab-to-lab basis.

Another concern raised by the participants was that biosecurity might result in restricting access to certain types of research. Sandia does not promote the idea of restricting publications of microbiological research. Information security should be applicable primarily to information that, if released, could result in facilitating an adversary's efforts at gaining access to the protected pathogens and toxins.

Physical Security

John Milloy, Ph.D., Sandia National Laboratories, United States

Physical security is one of six components of biosecurity. An individual laboratory may choose to incorporate a variety of features into their security system depending on the level of physical security its management believes is appropriate and the availability of resources. These features may be electronic in nature – including intrusion detection sensors, cameras, and biometric access controls – or non-electronic or manpower intensive, such as mechanical locks and the use of private guard forces. A facility could allocate extensive resources to physical security if management decided this level of protection were an efficient use of funding. Other labs may see no need for extensive controls and may be content with a much lower level of physical security.

Every country must make responsible decisions regarding physical security that ensure a balance between protecting their most dangerous pathogens and toxins with the limited resources available for security expenditures.

Physical security mechanisms by themselves are not enough to achieve biosecurity. These physical security mechanisms must be supported by personnel security, material control and accountability, material transfer security, information security, and program management.

Discussion

Although physical security can be a very expensive undertaking, most laboratories already have at least some level of "industrial security." They have locks on the doors and windows, and workers would most likely be aware of any specious and unauthorized person in a high-containment laboratory. At many facilities, this level of physical protection would be sufficient; at others, relatively minor increases in physical security may need to be applied.

Most existing industrial security mechanisms aim to protect the laboratory's expensive equipment such as computers. These physical security mechanisms are designed to protect against the outsider threat; they do not adequately provide sufficient protection against the laboratory insider. Since the insider is most often the threat of concern for a laboratory's dangerous pathogens and toxins, facilities with industrial security should only have to allocate a small amount of additional resources in order to achieve the physical security component of biosecurity.

It was agreed that some useless and wasteful physical security technologies have been applied to bioscience facilities. For example, video cameras focused on freezers cannot positively identify individuals wearing protective masks, and some motion-detecting sensors are susceptible to an unacceptable amount of false alarms.

Personnel Security

Natalie Barnett, M.S., Sandia National Laboratories, United States

Sandia has identified the laboratory "insider" as the primary threat to pathogens and toxins due to the fact that the insider has authorized access to and knowledge of high-risk pathogens. Therefore he or she may be able to not only divert assets without causing suspicion, but also effectively deploy that material as a weapon.

Personnel security aims to reduce the risk that an insider would steal or sabotage dangerous biological materials. Personnel security uses background investigations, badging, visitor controls, new employee orientations, and employee termination procedures to help deter or detect malicious actions taken by an insider.

It is important to note that not all positions within a high-containment laboratory require equal levels of scrutiny. Some positions are more sensitive than others, and the background investigation provided for those in high-risk positions should be more rigorous than for those in moderate- or low-risk positions. Visitor controls should

also vary depending on the level of access provided and the materials available to the visitor.

Discussion

Personnel security is a contentious subject for many researchers. The policies and procedures associated with personnel security may convey the message to the scientist that he or she or a co-worker is the primary threat, rather than some anonymous and fictitious "terrorist." Sometimes this can come as an unexpected shock. Also, some of the methods involved – especially background checks – may be interpreted by the researcher as degrading because they imply that he or she is not trustworthy.

The discussion focused primarily on the issue of background checks. Many participants regarded this vetting technique as too intrusive, too expensive, and too highly susceptible to error. Rather, psychological testing was expressed as a more commonly used and trusted screening tool for the hiring process. These tests are designed to evaluate an individual's personality and mental disposition, as well as to predict his or her compatibility within a research group or institution.

A concern was raised that the number of scientists certified to work with high-risk agents would be reduced through the investigation process itself – either by the individual refusing to be investigated or as the result of being rejected after not meeting a particular standard of conduct. There is a general sense that many scientists in the US are leaving work that is associated with regulated biological agents and toxins as a result of the impositions of the Select Agent Rule. However, there are no studies that confirm or dispel this belief.

Participants agreed that, after the hiring process, managers should be aware of any strange or dangerous behaviors displayed by their co-workers. Disenfranchised or emotionally disturbed workers with access to high-risk agents were generally agreed to pose a threat to the containment of a laboratory. However, most did not think this threat could be addressed with personnel security, but rather, that it was best addressed with attentive management practices.

Material Control and Accountability

George Baldwin, Ph.D., Sandia National Laboratories, United States

Material Control and Accountability (MC&A) is an integral component of the biosecurity system. MC&A provides timely and accurate knowledge of what materials exist at a laboratory facility, where those materials are, and who has access to them.

Dr. Baldwin emphasized that biosecurity "accountability" is *not* analogous to nuclear security "accountancy." Nuclear accountancy aims to provide a highly accurate, quantifiable account of the amount of nuclear material that is located at an exact

location. Biosecurity accountability does not attempt to quantify the exact amount of biological material in a facility; rather, it promotes a system that associates collections of material with specific persons who are accountable and responsible for the control and oversight of that material. Accountability reduces the risk of losing or misplacing critical biological material, but does not attempt to count each and every pathogen.

MC&A is achieved by conducting gross inventories – physically looking and recording what materials are where, and then continually updating those inventories when changes are made. Much of this is already done to maintain biosafety and good research and business practices.

Discussion

MC&A is already conducted at most laboratories throughout the world, albeit for reasons other than biosecurity. Therefore, the discussion focused on the inconsistencies within MC&A rather than whether or not it was a sound practice.

Most MC&A inconsistencies reside in how individual researchers record and track their materials. Because materials come in many different forms, drafting and using a standardized template is a difficult task. Luckily, computer programs are making standardization a much more achievable goal, while simultaneously reducing much of the operational burden associated with conducting and updating inventories.

It was mentioned that user-friendly computer databases already exist and are in use in some parts of the world. There was a general consensus that these technologies would make accountability a much easier task and should be shared, possibly through the WHO.

One weakness in the area of MC&A is the common laboratory problem of freezers containing unknown and usually historical samples. For instance, it is not uncommon for a researcher to retire and leave many of his microorganisms behind. Generations of scientists may pass through the laboratory, thereby leading to a complete loss of information associated with those materials. Still, there is a reluctance to discard these materials.

Transfer Security

Jennifer Gaudioso, Ph.D., Sandia National Laboratories, United States

Transfers occur every time a pathogen or toxin is removed from one containment area and delivered to another. This happens both within facilities (internal transfers) and between facilities (external transfers). Sandia believes that high-risk pathogens and toxins are vulnerable to theft during these processes. Therefore, laboratories should institute policies and procedures that help to secure these materials during the transfer process.

One practice laboratories should implement is a "chain of custody" for high-risk material transfers. Chain of custody refers to the procedures and documentation used to track who has control over material transfers between areas that are physically protected. Chain of custody ensures that only accountable and authorized individuals have physical control over the sample during its entire movement.

Discussion

Most of the discussion focused on the international transfer of infectious materials, which constitutes a problem for much of the world. Most countries have difficulties identifying a courier that will handle packages containing infectious materials. If and when a courier is identified, these companies often charge an exorbitant fee of several thousand dollars per package shipped. An additional problem encountered during transportation occurs when pilots exercise their right of refusal of any package they deem unsafe. Packages marked "Infectious Substance" have been reportedly abandoned on the tarmac after pilots have declined to load them on their airplanes.

The discussion highlighted how regulations stemming from one country can have unintended and far-reaching consequences in other countries. Currently, some US facilities require end-use agreements that place restrictions on what research may be conducted on certain agents, and prohibit the re-export of the material. This has vast implications for the WHO, which operates collaborative centers within the US and other countries. Because it WHO's policy to refuse to sign end-use agreements, collaborative centers in the US, which are subject to US law, are unable to share diagnostic samples with centers elsewhere. This impedes the international exchange of pathogens, especially diagnostic samples.

Information Management

Susan Caskey, M.S., Sandia National Laboratories, United States

All laboratories have and create vast amounts of information. This information can include laboratory reports, inventories, physical security plans, and human resource information. Some of this information, or aspects of it, should be considered sensitive and protected against release. Information management, as a component of biosecurity, includes the use of an information risk assessment to judge what information is considered sensitive, and determine which policies, procedures, and technologies are appropriate to protect this information. Just like pathogens, not all information requires the same level of protection. The highest levels of information protection should be imposed only for the protection of information that could directly lead to the loss of high-risk pathogens and toxins.

Information management is *not* the censorship of microbiological research. Rather, it protects the information that, if released, could facilitate the theft or sabotage of a high-risk pathogen or toxin. This information could include security-systems information (i.e. facility blue prints and lock combinations), human resource data, and detailed facility inventories.

Discussion

There were questions regarding how Select Agent research information is being protected within the US. Some US scientists and institutions are treating Select Agent research information as sensitive and are reluctant to share any data associated with these agents, especially with foreign nationals. The US Government, however, does not have any regulations that stipulate Select Agent research information is either sensitive or classified, and there are no plans to restrict Select Agent publications.

There is a general unease regarding the relationship of information security to the release of research information via publication or other public forms of data exchange. A number of participants raised the concern that implementing information security would lead to restrictions on what types of research could be conducted and which results shared.

Ms. Caskey gave a useful analogy that related the discovery of computer program vulnerabilities to the publishing of microbiological research advances. When software vulnerabilities are found, it is considered common practice to distribute this information via the Internet. That way, many independent programmers are afforded unimpeded access to the source code, and can work to develop a corrective patch. Similarly, in microbiology, discoveries that may lead to negative public health consequences should be openly distributed to researchers around the world so that solutions or countermeasures may be found.

Program Management

Natalie Barnett, M.S., Sandia National Laboratories, United States

All of the five components of biosecurity are brought together under the aegis of program management. The program management component of biosecurity is responsible for developing the laboratory's biosecurity and incident response plans, designing biosecurity training courses for employees, and allocating a laboratory's security resources. In addition, program management ensures the different elements of biosecurity – biosecurity methodology, physical security, personnel security, material control and accountability, transfer security, and information security – all work together with a high level of synergy.

Discussion

After a short discussion regarding where in a nation's bureaucratic structure biosecurity program management appropriately originates (national authorities or facility management), the discussion turned to the recurring theme of biosafety versus biosecurity.

The distinction between biosecurity and biosafety was unclear for many of the participants contributing to the symposium. Some participants thought that most of the issues brought up by Sandia had already been addressed either in the context of biosafety or under best business practices. Further, these participants thought that any issue not currently addressed by biosafety or best business practices could be incorporated into existing biosafety guidelines, rather than in a separate and new set of biosecurity-specific guidelines. Others in the group saw a clear distinction between the two disciplines, but recognized the need for coordination between biosecurity and biosafety policies and procedures.

The distinction between general security and biosecurity was raised. As previously stated, many laboratories have instituted "industrial" security to prevent the theft of goods with obvious monetary value. Those participants who interpreted a difference between general security and biosecurity suggested that the two, while related, had certain differences. Biosecurity focuses almost exclusively on preventing the theft of high-risk pathogens and toxins. It relies on a variety of strategies aside from physical security to achieve this goal; including personnel security, transfer security, and material accountability. General security, however, protects equipment, such as computers, from theft primarily using physical security measures. Also, effective and realistic biosecurity is promulgated from the scientific community and practiced by the individual researcher – much like biosafety. Alternatively, a guard force or the local police, who do not necessarily have training in microbiology, enforce general security.

The question of who should develop and disseminate biosecurity guidelines was raised. Participants discussed the viability of biosecurity standards modeled after the International Commission on Radiological Protection, which governs radiological safety standards, or the International Standards Organization, which normalize a variety of international standards. The WHO's role in promoting guidelines was also explored. Some participants suggested that no form of international guidelines or regulations should be developed, and that each country should independently decide on appropriate levels of biosecurity.

It was generally agreed that, if international biosecurity standards were to be drafted, the WHO would be the organization most trusted to publish and promulgate fair and balanced guidelines.

Friday, February 6

Friday's round-table discussions were an opportunity for participants to address any lingering questions or concerns they may still have had regarding biosecurity. The majority of topics during the session centered on four key subjects:

1) The fear that biosecurity would do more harm than good;
2) Most countries in the world have limited resources within their public health systems and must first and foremost address the immediate threat of endemic

infectious disease. Biosecurity, seen as a counter-biological terrorism tool, does not constitute a priority when allocating these scarce public health funds;
3) Biosecurity has already been achieved through a mixture of biosafety policies and good business, research, and management practices;
4) If international biosecurity is to become a global reality, the WHO is the only appropriate entity to promulgate guidelines.

There appears to be a general wariness regarding the implementation of biosecurity. Most participants attending the symposium expressed concern that biosecurity could become – and perhaps has become for the United States – a deterrent to microbiologists continuing their research on the most dangerous infectious diseases. Currently, there is no evidence to support or refute these claims; nevertheless the opinion exists.

Other fears held by some members of the international community include: the belief that biosecurity would lead to the censorship and classification of infectious disease research; that biosecurity would hinder international diagnostic transfers; and that the methods associated with the US Select Agent Rule – which is highly contentious – would be forced on other countries.

These fears have one common theme: Biosecurity could hinder necessary research on infectious diseases by diverting funds away from critical experiments and diagnostics. Endemic infectious disease is a much greater fear to the majority of the international community than the threat of bioterrorism. Infectious disease is an everyday occurrence in most of the world and its effects can be vastly destabilizing. Bioterrorism is seen more as a theoretical or extra-territorial concern and therefore the argument is made that it deserves less attention. Furthermore, the same techniques used to control natural outbreaks could be used to control a bioterror attack. Therefore, allocating resources to a field that only addresses the threat of bioterrorism is seen as an inefficient use of a nation's limited funds.

Some participants held the belief that biosecurity was a subset of biosafety, and that biosecurity could be achieved – or has already been achieved – through practices already in existence within most laboratories, especially those in the developed world.

Those who maintained there was a distinction between biosafety and biosecurity made the case that the two concepts addressed different risks. Biosafety concentrates on the accidental release of pathogens and toxins, while biosecurity addresses their intentional diversion. Because the risks are different, different but overlapping techniques must be applied to each to achieve both.

When posed the question of how biosecurity could be promoted internationally, most members of the symposium agreed that the only legitimate body able to promulgate guidelines would be the World Health Organization. Emphasis was made that "guidelines" could only be defined as a set of non-binding recommendations. There

is a concern that biosecurity, in the form of legally binding regulations, will be forced upon the international community.

It was the opinion of many participants that, if and when these guidelines are drafted, regional workshops should be conducted to help clarify and promulgate the new recommendations for the benefit of nations interested in instituting biosecurity.

Conclusion

The International Symposium on Securing High Consequence Pathogens and Toxins constituted an opportunity for a wide variety of nations to begin an international dialogue focused on biosecurity.

Much was accomplished during the week, but many issues were raised that require future consideration. For instance, there are legitimate fears that biosecurity could be a hindrance to infectious disease research. These fears must be addressed and alleviated by ensuring that biosecurity practices are commensurate with the bioterror threat and do not impede necessary laboratory work. Also, the WHO was almost unanimously chosen as the appropriate organization to draft and distribute biosecurity guidelines, but there remains the question of how the international community can best support this process.

Sandia National Laboratories believes that the symposium was a significant achievement and a promising beginning to further international collaboration on biosecurity.

Participant Register[4]

Australia

Tony Della Porta
Biosecurity and Biocontainment International Consultants Pty Ltd

Brazil

Pericles Palha de Oliveira
Ministry of Science and Technology

Czech Republic

Barbora Mackova
Czech National Collection of Type Cultures
National Institute of Public Heath

India

Ganga Prasad Rai
Defense Research and Development Establishment

Indonesia

Fransiscus Zaverius Suharyanto Halim
National Institute of Health Research and Development
Ministry of Health

Anne Kusmayati
Research and Development Agency
Department of Defense

Bambang Soebaygo
Research and Development Agency
Department of Defense

Japan

Tomoo Nagai
Ground Staff Office
Japan Defense Agency

[4] This list excludes those participants from Sandia National Laboratories.

Malaysia

Roslan bin Abd Aziz
Science and Technology Research Institute for Defense
Ministry of Defense

Lt. Col. Zulkifibin Ahmad
Policy Division
Ministry of Defense

Poland

Marek K. Janiak
Military Institute of Hygiene and Epidemiology

Hanusz Kocik
Military Institute of Hygiene and Epidemiology

South Africa

Ben Steyn
South African Military Health Service

South Korea

Kidong Park
Health Promotion Bureau
Ministry of Health and Welfare

Won Keun Seong
Research Center for Pathogen Control
Department of Bacteriology
National Institute of Health

Thailand

Chalinee Kongsaway
Biosafety Program
National Center for Genetic Engineering and Biotechnology

United Kingdom

Darrel Barber
National Counter Terrorism Security Office

Guy Collyer
National Counter Terrorism Security Office

Andrew Cottam
Biological Agent Unit
Health and Safety Executive

Lorna Miller
Porton Down

World Health Organization

Bradford Kay
Communicable Disease Surveillance & Response,
World Health Organization

United States

Matthew Axelrod
Biological Weapons Proliferation Prevention
Defense Threat Reduction Agency
Department of Defense

Thomas E. Bevan
Center for Emergency Technology, Instruction, and Policy
Georgia Institute of Technology
Georgia Tech Research Institute

Elizabeth Cameron
Office of Proliferation Threat Reduction
Department of State

Michael Congdon
Office of Nonproliferation Policy
National Nuclear Security Administration
Department of Energy

Michel Dahlstrom
Lawrence Livermore National Laboratory

Nelson Erickson
Office of the Assistant Secretary of Defense
Department of Defense

Scott Filer
Argonne National Laboratory

John-Olav Johnson
National Nuclear Security Administration,
Department of Energy

Michael Moodie
Chemical and Biological Arms Control Institute

Keith Murray
National Animal Disease Center,
Agricultural Research Service,
Department of Agriculture

Janet K.A. Nicholson
National Center for Infectious Diseases
Centers for Disease Control and Prevention
Department of Health and Human Services

Myron Oden
Office of Security and Emergency Preparedness
Centers for Disease Control and Prevention
Department of Health and Human Services

Tara O'Toole
Center for Biosecurity
University of Pittsburgh Medical Center

Lt. Col. Ross Pastel
US Army Medical Research Institute of Infectious Diseases

William Porter
Office of Security and Emergency Preparedness
Centers for Disease Control and Prevention
Department of Health and Human Services

Michael Powers
Chemical and Biological Arms Control Institute

Douglas J. Pruett
Office of Security and Drug Testing
Department of Health and Human Services

Guy Roberts
OSD Negotiations Policy
Department of Defense

Gregory Stewart
Office of Chemical and Biological Weapons Conventions
Bureau of Arms Control
Department of State

Jill Trewhella
Bioscience Division
Los Alamos National Laboratory

Richard Weller
Pacific Northwest National Laboratory

Symposium Agenda

Securing High Consequence Pathogens and Toxins

International Security Center
Sandia National Laboratories

Albuquerque, New Mexico, USA
February 1-6, 2004

Points of Contact

Technical Host:	Reynolds Salerno
Symposium Coordinator:	Lauren Hickok
International Protocol:	Evangeline Clemena

Sunday, February 1

Opening Events – Sheraton Uptown Hotel

15:00 – 17:00	Registration	Lobby Area
17:30 –18:00	Opening Reception	Galleria Room
18:00 – 20:30	Opening Dinner	Baldwin Room
	Host	Reynolds Salerno *Sandia National Laboratories*
	Sandia National Laboratories Welcome	Al Romig, Vice President *National Security and Arms Control Division* *Sandia National Laboratories*
	Introductory Comments	Michael Congdon *U.S. Department of Energy* Gregory Stewart *U.S. Department of State* Guy Roberts *U.S. Department of Defense* William Porter *US Centers for Disease Control and Prevention* Bradford Kay *World Health Organization*

Monday, February 2

Breakfast – IPB Room 1151

7:30 – 8:00	Breakfast	

Symposium Group Photo – IPB Front Entrance

8:00 – 8:40	Group Photo	

Badging – IPB Room 1154 - 1155

8:40 – 9:10	Badging at Sandia National Laboratories	

Symposium Introduction – IPB Room 1154 – 1155

9:10 – 9:40	Sandia National Laboratories Introduction	Dori Ellis, Director *International Security Center* *Sandia National Laboratories*
9:40 – 9:50	International Symposium Overview	Reynolds Salerno *Sandia National Laboratories*
9:50 – 10:20	Participant Introductions	

Session One: The Threat – IPB Room 1154 – 1155

10:20 – 11:00	Historical Trends and the Biological Weapons Threat	Michael Moodie *Chemical and Biological Arms Control Institute*
11:00 – 11:40	The Biotechnology Revolution and the Biological Weapons Threat	Tara O'Toole *Center for Biosecurity of the University of Pittsburgh Medical Center*

Session Two: Biological Weapons Nonproliferation – IPB Room 1154 – 1155

11:40 – 12:20	Pathogen Security and the Biological Weapons Convention	Gregory Stewart *Bureau of Arms Control* *Office of Chemical and Biological Weapons* *U.S. Department of State*

Lunch – IPB Room 1151

12:20 – 13: 20	Lunch	

Monday, February 2 (continued)

Session Two Cont: Biological Weapons Nonproliferation – IPB Room 1154 – 1155

13:20 – 14:00	Options for Reducing the Threat	Elizabeth Cameron *Bureau of Nonproliferation* *Office of Proliferation* *Threat Reduction* *U.S. Department of State*

Session Three: Responses to the Threat – IPB Room 1154 – 1155

14:00 – 14:40	Biomedical Countermeasures	Lt. Col. Ross Pastel *U.S. Army Medical Research* *Institute of Infectious Diseases*
14:40 – 15:20	Veterinary Infectious Diseases, New Technologies and the Future	Keith Murray *National Animal Disease Center* *Agricultural Research Service* *U.S. Department of Agriculture*

Break – IPB Room 1151

15:20 - 15:40 Break

Session Three Cont: Responses to the Threat – IPB Room 1154 – 1155

15:40 – 16:20	Bio-Forensics	Jill Trewhella *Los Alamos National Laboratories*
16:20 – 17:00	Next Generation Biosensors	Thomas Bevan *Georgia Institute of Technology*

Dinner – Albuquerque Land and Cattle Co.

19:00 – 21:00 Dinner

Tuesday, February 3

Breakfast – IPB Room 1151

7:30 – 8:00	Breakfast	

Session One: Biosecurity in Practice Internationally – IPB Room 1154 – 1155

8:00 – 8:30	'Biosecurity:' The United Kingdom's Response	Guy Collyer *National Counterterrorism Security Office* *United Kingdom*
8:30 – 9:00	Integrated Biological Attack Response System in Poland: Model and Reality	Janusz Kocik *Military Institute of Hygiene and Epidemiology* *Poland*
9:00 – 9:30	Biological Threats and Biosecurity Efforts in Indonesia	Fransiscsus Xaverius Suhuryanto Halim *National Institute of Health Research and Development, Ministry of Health* *Indonesia*

Break – IPB Room 1151

9:30 – 10:00	Break	

Session One Cont: Biosecurity in Practice Internationally – IPB Room 1154 – 1155

10:00 – 10:30	South Africa: Biosecurity Presentation	Ben Steyn *South African Military Health Service* *South Africa*
10:30 – 11:00	Australia: Biosecurity and Biosafety Practices	Antony Della-Porta *Biosecurity and Biocontainment International Consultants*
11:00 – 11:30	Implementation of Biosecurity in the United States	Janet Nicholson *National Center for Infectious Disease* *Centers for Disease Control and Prevention* *United States*

Lunch – IPB Room 1151

11:30– 12:30	Lunch	

Tuesday, February 3 (continued)

Session One Cont: Biosecurity in Practice Internationally – IPB Room 1154 – 1155

12:30 – 14:00	International Biosecurity Panel Discussion	Richard Weller, co-moderator *Pacific Northwest National Laboratory* Michael Moodie, co-moderator *Chemical and Biological Arms Control Institute*

Session Two: Poster Session – IPB Display Area

14:00– 17:00	Poster Presentations

Dinner – Japanese Kitchen

19:00 – 21:00	Dinner

Wednesday, February 4

Breakfast – IPB Room 1151

7:30 – 8:00	Breakfast	

Session One: Biosecurity – IPB Room 1154 – 1155

8:00 – 9:00	Biosecurity Methodology	Reynolds Salerno *Sandia National Laboratories*
9:00 – 9:30	Discussion of Biosecurity Methodology	
9:30 – 10:00	Break	

Session Two: Physical Security – IPB Room 1154 – 1155

10:00 – 11:00	Physical Security	John Milloy *Sandia National Laboratories*
11:00 – 12:00	Physical Security Discussion	

Lunch – IPB Room 1151

12:00 – 13:00	Lunch	

Session Three: Personnel Security – IPB Room 1154 – 1155

13:00 – 14:00	Personnel Security	Natalie Barnett *Sandia National Laboratories*
14:00 – 15:00	Personnel Security Discussion	
15:00 – 15:30	Break	

Session Four: Material Control and Accountability – IPB Room 1154 – 1155

15:30 – 16:30	Material Control and Accountability	George Baldwin *Sandia National Laboratories*
16:30 – 17:30	Material Control and Accountability Discussion	

Dinner – Scalo Italian Grill

19:00 – 21:00	Dinner	

Thursday, February 5

Breakfast – IPB Room 1151

7:30 – 8:00	Breakfast	

Session One: Transfer Security – IPB Room 1154 – 1155

8:00 – 9:00	Transfer Security	Jennifer Gaudioso *Sandia National Laboratories*
9:00 –10:00	Transfer Security Discussion	

Break – IPB Room 1151

10:00 – 10:30	Break	

Session Two: Information Security – IPB Room 1154 – 1155

10:30 –11:30	Information Security	Susan Caskey *Sandia National Laboratories*
11:30 –12:30	Information Security Discussion	

Lunch – IPB Room 1151

12:30 – 13:30	Lunch	

Session Three: Program Management – IPB Room 1154 – 1155

13:30 – 14:30	Program Management	Natalie Barnett *Sandia National Laboratories*
14:30 – 15:00	Program Management Discussion	

Break / Albuquerque Tour – Old Town

15:00 – 18:00	Break/Albuquerque Tour	

Dinner – La Placita

19:00 – 21:00	Dinner	

Friday, February 6

Breakfast – IPB Room 1151

7:30 – 8:00	Breakfast	

Roundtable Discussion – IPB Room 1154 – 1155

8:00 – 12:00	Questions and Answers	Reynolds Salerno, moderator *Sandia National Laboratories*

Lunch – IPB Room 1151

12:00 – 13:00	Lunch
13:00	Adjourn